A Generalization of Wilson's Theorem

R. Andrew Ohana

June 3, 2009

Contents

1 Introduction

In 1770 Edward Waring published the text *Meditationes Algebraicae*, in which several original statements in number theory were formed. One of the most famous was what is now referred to as Wilson's Theorem - named after the student who made the conjecture, John Wilson - which states that all primes p divide $(p-1)!+1$. No proof was originally given for the result, as Wilson left the field of mathematics quite early to study law, however the same year in which it was published, J. L. Lagrange gave it proof. In this paper, we will cover the necessary algebra, a proof of Wilson's Theorem, and a proof of Gauss' generalization of Wilson's Theorem. Finally, we'll conclude with a brief discussion of Wilson primes, primes that satisfy a stronger version of Wilson's Theorem.

2 Background Algebra

In order to discuss Wilson's Theorem, we will need to develop some background in algebra. Nearly all the proofs in this section will be left for the reader, for more on basic algebra consult [1], [2], or [4].

2.1 Groups

Much of algebra builds off of the idea of a group. The idea is rather basic, given a set and an operator - such as multiplication or addition - the pair is a group if there is closure and associativity. By closure we mean that if x and y are in the set, then $x \cdot y$ and x^{-1} are in the set, where $\cdot$ is our operator. Thus we arrive to our formal definition of group.

Definition 2.1.1. *A **group** G is a set along with an operator "multiplication," denoted by $\cdot$, such that*

1. *for all $x, y \in G$, $x \cdot y \in G$,*
2. *for all $x, y, z \in G$, $x \cdot (y \cdot z) = (x \cdot y) \cdot z$,*
3. *there exists an $e \in G$ such that for all $x \in G$, $x \cdot e = e \cdot x = x$,*
4. *for all $x \in G$, there exists an $x^{-1} \in G$ where $x \cdot x^{-1} = x^{-1} \cdot x = e$.*

It is convention to denote $a \cdot b$ as ab. A few basic properties follow directly from the definition of a group.

Theorem 2.1.2. *Let G be a group, then*

1. *for all $x, y, z \in G$, if $xy = xz$, then $y = z$.*
2. *for all $x, y, z \in G$, if $xy = zy$, then $x = z$.*
3. *the identity element e is unique.*

4. the inverse x^{-1} is unique.

Note that commutativity is not required in a group, we call a group abelian if all its elements commute.

Definition 2.1.3. *A group G is **abelian** if $xy = yx$ for all $x, y \in G$.*

In this paper we will discuss only abelian groups.

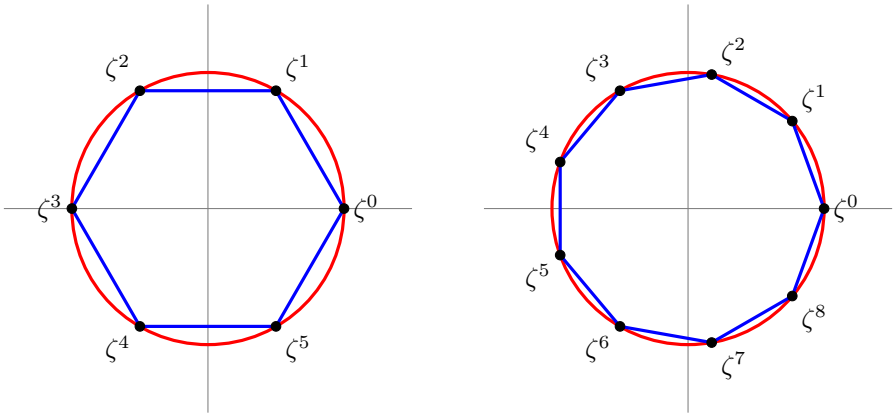
Next, we would like to have the ability of generating a group. By this we mean that if we look at an element, and apply an operator repetitively to it, we create a group. We define

$$\begin{aligned} x^0 &= e, \\ x^n &= \underbrace{x \cdots x}_{n \text{ times}}, \\ x^{-n} &= \underbrace{x^{-1} \cdots x^{-1}}_{n \text{ times}}, \end{aligned}$$

which we can easily verify behaves in the way we expect exponents to behave.

Example 2.1.4. Consider $\zeta = e^{2\pi i/n}$ and the operator of multiplication, then ζ generates the group of the n-th roots of unity, $G = \left\{\zeta^k : 0 \leq k < n\right\}$.

1. We have closure under multiplication: for all $x, y \in G$, $xy \in G$.
2. We have associativity: for all $x, y, z \in G$, $x(yz) = (xy)z$.
3. We have identity element 1: for all $x \in G$, $x \cdot 1 = 1 \cdot x = x$.
4. We have closure under inverses: for all $x \in G$, $x(x^{n-1}) = (x^{n-1})x = 1$.



(a) The 6th roots of unity.

(b) The 9th roots of unity.

Figure 1: Examples of the n-th roots of unity.

In general, when we consider a group generated by an element x we have the set $\left\{e, x, x^2, x^3, \ldots, x^{-1}, x^{-2}, x^{-3}, \ldots\right\}$. This leads us to the idea of a cyclic group.

Definition 2.1.5. *A group G is **cyclic** if there exists an $x \in G$ such that for all $y \in G$, $y = x^n$ for some $n \in \mathbb{Z}$. We call x a generator of G.*

Example 2.1.6. Consider the integers under addition

1. We have closure under addition: for all $m, n \in \mathbb{Z}$, $m + n \in \mathbb{Z}$.
2. We have associativity: for all $m, n, q \in \mathbb{Z}$, $m + (n + q) = (m + n) + q$.
3. We have identity element 0: for all $n \in \mathbb{Z}$, $n + 0 = 0 + n = n$.
4. We have closure under inverses: for all $n \in \mathbb{Z}$, $n + (-n) = (-n) + n = 0$.
5. We have commutativity: for all $m, n \in \mathbb{Z}$, $m + n = n + m$.

Hence the integers are an abelian group. In addition we have that the integers are a cyclic group since $1^n = n$, for $n \in \mathbb{Z}$.

Notice how the integers are both abelian and cyclic, we actually have something stronger.

Theorem 2.1.7. *All cyclic groups are abelian.*

The converse however is not true, we can note this by considering the rationals under addition, for the same reasons we have that $\mathbb{Q}$ is abelian, but note that we cannot find a generator for the group.

Next we would like a notion of size. Notice, that while there are an infinite number of integers, which form a group, we saw in Example 2.1.4 that we had a group with only a finite number of elements (namely n). This leads us into the order of a group.

Definition 2.1.8. *The **order** of a group G, denoted $|G|$, is the number of elements in G.*

Similarly, we have for elements in a group a definition of order.

Definition 2.1.9. *The **order** of an element $x \in G$ is the minimum natural n such that $x^n = e$.*

Hence for the group of integers is infinite order since there are an infinite number of elements, in addition every non-zero element has infinite order since there is no power k in for which $n^k = 0$ when $n \neq 0$. On the other hand, the n-th roots of unity have order n, and have at least one element of order n, the generator.

Finally, we will introduce the idea of a subgroup.

Definition 2.1.10. *Let G be a group, a **subgroup** H is a subset of G such that H is a group. We denote this relation as $H < G$.*

Example 2.1.11. Consider the integers, $\mathbb{Z}$, and the multiples of n, $n\mathbb{Z}$. Clearly $n\mathbb{Z} \subseteq \mathbb{Z}$, we also have that $n\mathbb{Z}$ is a group (since we have closure, associativity, and the identity element). Thus $n\mathbb{Z} < \mathbb{Z}$.

2.2 Rings

The idea of a ring extends the idea of group. Here we are able to talk about integers in their full capacity, including both addition and multiplication. To do this, we extend an abelian group and add a second operator. This second operator does not have the strict of restrictions of the first operator, in fact all that is required is closure under the operator, associativity, and a distribution law with respect to the first operator.

Definition 2.2.1. *A **ring** R is a set along with on operators "addition" and "multiplication," denoted by $+$ and $\cdot$ respectively, such that under addition the set forms an abelian group denoted R^+, and for all $x, y, z \in G$*

1. $x \cdot y \in R$,
2. $x \cdot (y \cdot z) = (x \cdot y) \cdot z$,
3. $x \cdot (y + z) = x \cdot y + x \cdot y$ *and* $(x + y) \cdot z = x \cdot z + y \cdot z$.

Again, it is convention to denote $a \cdot b$ as ab. In addition it is convention to denote the identity element of R^+ as 0 instead of e. Consider the integers again, we already know that 0 is the identity element of R^+, but now consider 1, we have that $n \cdot 1 = n \cdot 1 = n$ for all $n \in \mathbb{Z}$. This brings us to the idea of rings with identity.

Definition 2.2.2. *A ring is with **identity** if there exists an element $1 \in R$ such that $0 \neq 1$ and for all $x \in R$, $x \cdot 1 = 1 \cdot x = x$.*

Note that 1 in the definition is not to be confused with the number 1, although frequently the two correspond, hence the notation. If we continue to follow our example of the integers, we note that only two elements (namely 1 and -1) have multiplicative inverses. This idea generalizes to the idea of a unit - whose terminology stems from the fact that 1 and -1 have magnitude 1.

Definition 2.2.3. *Let R be a ring with identity, a **unit** is an element $x \in R$ for which there exists $x^{-1} \in R$ where $xx^{-1} = x^{-1}x = 1$.*

Theorem 2.2.4. *Let R be a ring with identity, the set of units in R form a group under multiplication. We denoted this group as $R^\times$.*

Example 2.2.5. Consider $M_n(\mathbb{R})$, the set of $n \times n$ matrices with real number entries. We can see that under addition, we clearly have that $M_n(\mathbb{R})^+$ is an abelian group with 0 being the zero-matrix. It can be easily verified that $M_n(\mathbb{R})$ is associative under multiplication, and that the distribution property holds. Now consider the identity matrix, clearly it is the multiplicative identity element, hence $M_n(\mathbb{R})$ is a ring with identity. Finally, note that the units of $M_n(\mathbb{R})$ are the invertible $n \times n$ matrices (which is usually denoted $GL_n(\mathbb{R})$ and is a rather important group in algebra).

Now we return to the idea of commutativity. Recall when discussing groups, we called a group abelian if all its elements commuted, similarly we have that a ring is commutative if all its elements commute under multiplication.

Definition 2.2.6. *A ring R is **commutative** if $xy = xy$ for all $x, y \in G$.*

Hence, we see that the integers form a commutative ring with identity. Where as on the other hand $M_n(\mathbb{R})$ is a ring with identity, but it is not commutative. Finally, we consider a special subset of a commutative ring.

Definition 2.2.7. *Let R be a commutative ring, an **ideal** I is a subset of R for which $I < R^+$ and for all $x \in I$ and $y \in R$, $xy \in I$.*

Example 2.2.8. Again consider the integers, $\mathbb{Z}$, and the multiples of n, $n\mathbb{Z}$. We already know from Example 2.1.11 that $n\mathbb{Z} < \mathbb{Z}^+$, thus consider $m \in \mathbb{Z}$ and $q \in n\mathbb{Z}$. Clearly we have $mq \in n\mathbb{Z}$, hence $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$.

If we consider all the multiples of an element in a ring, we can create an ideal, hence we have the theorem.

Theorem 2.2.9. *Let R be a ring and $x \in R$, then the set $(x) = \{xy : y \in R\}$ is an ideal. We call (x) the **principle ideal** generated by x.*

Example 2.2.10. From our definition of $n\mathbb{Z}$ in Example 2.1.11 we clearly have that $n\mathbb{Z} = (n)$.

2.3 Quotient Rings

Based off of what we have covered, it is difficult to produce examples of finite rings, therefore we need to introduce the idea of a quotient ring.

Theorem 2.3.1. *Let I be an ideal of a commutative ring R, then the set $R/I = \{x + I : x \in R\}$, where $x + I = \{x + y : y \in I\}$, is a ring. We call such rings **quotient rings**.*

Example 2.3.2. Consider $\mathbb{Z}$ and (n), then we know $\mathbb{Z}/(n) = \{m + (n) : m \in \mathbb{Z}\}$ is a ring. To get an idea of what this ring looks like, consider an element $k + (n)$ and $k + n + (n)$, we know $k + (n) = \{k + q : q \in (n)\}$ and that $k + n + (n) = \{k + n + q : q \in (n)\}$. Since $n + q \in (n)$, we know that $k + n + (n) = \{k + q : q \in (n)\} = k + (n)$. This follows the laws of modular arithmetic that we already know. Generally instead of denoting an element of $\mathbb{Z}/(n)$ by $k + (n)$, we drop the (n) and generally denote it by k.

2.4 Homomorphisms and Isomorphisms

To compare rings in a well defined fashion, we need to discuss relationships between them. Hence we define a homomorphism.

Definition 2.4.1. *Let R, R' be rings and $f : R \mapsto R'$, be a function that has the following properties:*

1. *For all $x, y \in R$, $f(x + y) = f(x) + f(y)$.*
2. *For all $x, y \in R$, $f(xy) = f(x)f(y)$.*

3. *If R, R' have identity, then $f(1_R) = f(1_{R'})$.*

*We call f a **ring homomorphism**.*

If we want to describe equivalence among rings R and R' we would like for the two act in the exact same manner. It can be shown that if there exists a bijective ring homomorphism $f : R \mapsto R'$, then the two rings behave the same.

Definition 2.4.2. *Let R, R' be rings, if there exists a bijective ring homomorphism $f : R \mapsto R'$, then R and R' are said to be **isomorphic**.*

2.5 Fields

The idea of a field extends the idea of ring. We have already fully developed the idea the integers, however we still can still develop the rationals. For example, when it comes to rings, we would like to avoid the idea of division since many elements don't have multiplicative inverses, however when dealing with the rationals, it is almost unnatural not to talk about division. Hence, we would like a construct which has the property that every non-zero element has a multiplicative inverse (like the rationals and the reals), this leads us to our definition of fields.

Definition 2.5.1. *A **field** K is a commutative ring with identity where all non-zero elements of K are units.*

For the next example, we need Bézout's Lemma.

Bézout's Lemma. *Let a and b be integers, and $(a, b) = d$, then there exist integers x and y such that $ax + by = d$.*

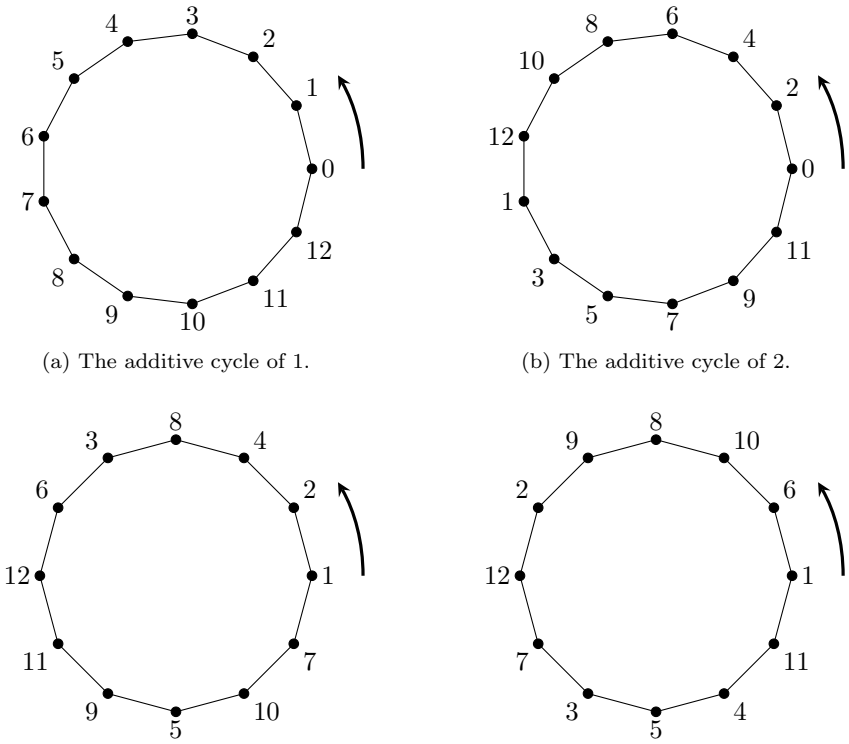
Example 2.5.2. Consider $\mathbb{Z}$ and (p), where p is prime. We already know $\mathbb{Z}/(p)$ is a ring, we now want to show that it is in fact a field. Let $n \in \mathbb{Z}/(p)$ be non-zero, since p is prime and $n < p$, we know $(n, p) = 1$. Hence by Bézout's Lemma we know their exist integer solutions for x and y to the equation $nx + yp = nx = 1$. Thus n has an inverse, and therefore n is a unit. Ergo $\mathbb{Z}/(p)$ is a field.

While at first look this may not seem like a very restrictive definition, the results we gain are quite significant. We will specifically be looking at finite fields, ones in which there are a finite number of elements. For finite fields, we have

Theorem 2.5.3. *Let p be a prime, and $q = p^\alpha$ be a prime power, then*

1. *there exists a field of order q.*
2. *all fields of order q are isomorphic.*
3. *if $|K| = q$, then $K^\times$ is a cyclic group of order $q - 1$.*

Since all finite fields of the same order act the same, we denote the unique finite field of order q as $\mathbb{F}_q$. Notice that from Example 2.5.2 we have already found $\mathbb{F}_p$ where p is prime. While we have found $\mathbb{F}_p$, we have not found $\mathbb{F}_q$ by the following theorem.



(a) The additive cycle of 1.

(b) The additive cycle of 2.

(c) The multiplicative cycle of 2.

(d) The multiplicative cycle of 6.

Figure 2: The structure of $\mathbb{Z}/(13)$.

Theorem 2.5.4. *The quotient ring $\mathbb{Z}/(n)$ is a field if and only if n is prime.*

Proof. By Example 2.5.2 we only need to show that if n is not prime, then $\mathbb{Z}/(n)$ is not a field. Suppose that n is composite and that $\mathbb{Z}/(n)$ is a field, then we know there exists a, b such that $n = ab$ and $1 < a, b < n$. In addition, we know there exists a^{-1} and b^{-1}, thus since $ab = 0$ we have $aba^{-1}b^{-1} = 1 = 0 = 0 \cdot a^{-1}b^{-1}$. But this is a contradiction since $0 \neq 1$, hence $\mathbb{Z}/(n)$ is not a field. □

In this paper, we only have the need for finite fields of prime order, for examples of other finite fields, consult [1], [2], or [4].

2.6 Polynomials

Now that we have developed through the idea of a field, we may begin to talk about more general polynomials. To start off with we have a theorem.

Theorem 2.6.1. *Let R be a ring, and consider the set $R[x]$ of functions of the form*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots a_1 x + a_0,$$

*where $a_i \in R$, $n \in \mathbb{Z}^{\geq 0}$, and x is a variable in R. The set $R[x]$ is a ring, which we call the **polynomial ring** over R.*

Example 2.6.2. Let $R = \mathbb{Z}/(2)$, then some sample arithmetic in $R[x]$ is

$$(x+1) + (x^2 + x + 1) = x^2$$
$$(x^2+1) + (x^2 + x) = x + 1.$$

For the most part, our discussion will be on polynomial rings over fields, denoted as $K[x]$. To start with our study of polynomials, we need to find the units of $R[x]$.

Theorem 2.6.3. *The units of $R[x]$ are the units of R.*

In other words, the constant functions which are units in R are the units in $R[x]$. When studying polynomials over fields we talk about the factorization of polynomials.

Definition 2.6.4. *An **irreducible** polynomial $f(x) \in K[x]$ has the property that if $f(x) = g(x)h(x)$, where $g(x), h(x) \in K[x]$, then either $g(x)$ or $h(x)$ are units.*

In the sense that primes form a primitive factorization for integers, we have irreducible polynomials forming a primitive factorization for polynomials.

Theorem 2.6.5. *Let $f(x) \in K[x]$ and let $f(x) = p_1(x)p_2(x)\cdots p_n(x)$ be a factorization into irreducibles $p_1(x), p_2(x), \ldots, p_n(x)$, then the factorization is unique up to a unit.*

This allows us to study all polynomials over a field, by studying just the irreducible polynomials. Finally, we need the definition of a root.

Definition 2.6.6. *Let $f(x) \in R[x]$ and $\alpha \in R$. If $f(\alpha) = 0$ then we call α a **root** of $f(x)$.*

2.7 Chinese Remainder Theorem

While more of a number theoretic result, the Chinese remainder theorem can help in finding roots to very specific polynomials in $\mathbb{Z}/(n)[x]$.

Theorem 2.7.1 (Chinese Remainder Theorem)**.** *Suppose that $n_1, n_2, \ldots, n_k$ are positive integers which are pairwise relatively prime. Then, for any given integers $a_1, a_2, \ldots, a_k$ there exists an integer α which is a simultaneous root to each $f_i(x) = x - a_i$ in $\mathbb{Z}/(n_i)$.*

This result is necessary for Gauss' Generalization of Wilson's Theorem.

3 Wilson's Theorem and Gauss' Generalization

Wilson's Theorem is a peculiar result in number theory which has only two major results. Firstly it serves as a primality test which is less efficient than a brute force divisor test. Secondly, and undoubtedly the more important result, is that it has as a corollary the famous result in quadratic residues which states -1 is a square $\bmod p$ if $p \equiv 1 \pmod 4$. While its results aren't very significant, it is an interesting curiosity in its own right, and has lead to the unsolved problem of Wilson primes.

3.1 Wilson's Theorem

Here we will give proof of Wilson's Theorem in its original form.

Theorem 3.1.1 (Wilson's Theorem)**.** *A positive integer $n > 1$ is prime if and only if $(n-1)! + 1$ is divisible by n.*

Proof. We will first suppose that n is prime. Consider the polynomial $f(x) = x^{p-1} - 1$ inside $\mathbb{F}_p[x]$ where p is an odd prime. By Theorem 2.5.3 we know that for each non-zero $\alpha \in \mathbb{F}_p$, that $\alpha^{p-1} = 1$, since $\mathbb{F}_p^\times$ is cyclic. Hence the roots of $f(x)$ are $1, 2, \ldots, p-1$, and thus we have the factoring

$$f(x) = x^{p-1} - 1 = \prod_{k=1}^{p-1} (x - k).$$

Evaluating $f(0)$ we find $-1 = (p-1)!$ in $\mathbb{F}_p$, hence $(p-1)! + 1$ is divisible by p. If $p = 2$, then we have $(2-1)! + 1 = 2$ which is divisible by 2.

Now we will prove the converse. Suppose that n is composite, then we have two cases, either $n = p^2$ for some prime p, or $n = ab$ where $1 < a < b < n$. First suppose the second, since $n > 2$ we know $b < n - 1$, hence we have $a \mid (n-1)!$ and $b \mid (n-1)!$. This gives us $n \mid (n-1)!$, which implies $(n-1)!+1$ is not divisible by n. Now suppose $n = p^2$ for some prime p. If $n = 4$, then $(4-1)! + 1 = 7$ which is not divisible by 4, so suppose $n > 4$. Since $p > 2$, we know $2p < n - 1$, and therefore $p \mid (n-1)!$, $2p \mid (n-1)!$, and $n \mid 2p^2$. This gives us $n \mid (n-1)!$, which implies $(n-1)! + 1$ is not divisible by n. □

3.2 Gauss' Generalization

Gauss noted that Wilson's Theorem was actually a special case of a more general theorem about all positive integers. Gauss' generalization of Wilson's Theorem states that if n is four, an odd prime power, or twice an odd prime power, then the product of relatively prime integers less than itself add one is divisible by n. In addition, it states that otherwise, the same product subtract one is divisible by n. We can see that this is a generalization of Wilson's Theorem, by observing how when n is a prime, the product is simply $(n-1)!$.

In order to state Gauss' generalization of Wilson's Theorem, we need to define Euler's totient function.

Definition 3.2.1 (Euler's Totient Function)**.** ***Euler's totient function****, denoted by $\varphi(n)$, is defined to be the number of positive integers less than or equal to n which are relatively prime with n.*

Theorem 3.2.2 (Gauss' Generalization)**.** *Let p be an odd prime and α be a positive integer, then in $\mathbb{Z}/(n)$*

$$\prod_{k=1}^{\varphi(n)} a_k = \begin{cases} 0 & n = 1, \\ -1 & n = 4,\ p^\alpha,\ 2p^\alpha, \\ 1 & \text{otherwise}, \end{cases}$$

where each a_i is a distinct positive integer less to or equal to n which is relatively prime with n.

Proof. Our proof is based off of the proofs given in [5] and [6]. For $n = 1$ and $n = 2$, the result is immediate, so assume $n > 2$. Since $(a_i, n) = 1$, we know there exists an a_j such that

$$a_i a_j = 1. \tag{$\dagger$}$$

Hence whenever $i \neq j$, we can pair terms together. Now consider the polynomial $f(x) = x^2 - 1$ in $\mathbb{Z}/(n)[x]$, clearly $i = j$ if and only if a_i or a_j is a root of $f(x)$. If a_i is a root of $f(x)$, then because $n > 2$, $n - a_i$ is also a root. Let Q_1 denote the product of the roots of $f(x)$. We wish to show that unless $n = 4$, $n = p^\alpha$, or $n = 2p^\alpha$, the number of roots is divisible by four. We start by considering $n = p^\alpha$, then by factoring

$$f(x) = (x - 1)(x + 1)$$

we find that there are exactly two roots. Now consider $n = 2$, then we notice that since $1 = -1$, there is a single root. Next consider $n = 4$, again we clearly have 2 solutions. Finally consider $n = 2^\beta$, $\beta > 2$, if one of the factors of $f(x)$ is divisible by 2, so is the other, but only one of them can be divisible by 4 or a higher power of 2. Hence if $x + 1$ is divisible by 2 only to the first power, we must have that 2 is a root of $f(x)$ in $\mathbb{Z}/(2^{\beta-1})$. This represents two different roots $x = 1$ and $x = 1 + 2^{\beta-1}$ of $f(x)$ in $\mathbb{Z}/(n)$. Similarly, when $x - 1$ contains only the first power of 2, we find the roots $x = -1$ and $x = -1 - 2^{\beta-1}$. Hence we can easily verify these four roots are distinct. Finally, we consider a general n by writing it in terms of its prime factors

$$n = 2^\beta p_1^{\gamma_1} \cdots p_r^{\gamma_r}$$

and finding the roots of $f(x)$ in $\mathbb{Z}/(2^\beta)$ and $\mathbb{Z}/(p_i^{\gamma_i})$. The Chinese remainder theorem shows that the roots of $f(x)$ is $\mathbb{Z}/(n)$ are obtained by selecting a particular root for each of the prime powers and finding the roots of $f(x)$ in each of $\mathbb{Z}/(p_i^{\gamma_i})$ simultaneously. When n is not divisible by 2, each of the equations have two roots so we obtain a total of 2^r roots. When $\beta = 1$, in $\mathbb{Z}/(2)$ we have a single root, so we will still have 2^r roots. When $\beta = 2$, in $\mathbb{Z}/(4)$ we have two roots, and so the total number in this case is 2^{r+1}. Finally, when $\beta > 2$, in

$\mathbb{Z}/(2^\beta)$ there are four roots so the total number of roots is 2^{r+2}. Thus, unless $n = 4$, $n = p^\alpha$, or $n = 2p^\alpha$, the number of roots is divisible by four. Now, note that if a_i is a root of $f(x)$, then

$$a_i(n - a_i) = -a_i^2 = -1.$$

Hence if the number of roots of $f(x)$ are divisible by four then $Q_1 = 1$, otherwise, $Q_1 = -1$. Now let Q_2 be the product of a_i's which aren't roots of $f(x)$, or if there are no such a_i's let $Q_2 = 1$. By (†) we can clearly see that if such a_i's exist then $Q_2 = 1$. Therefore we always have $Q_2 = 1$. Finally note

$$\prod_{k=1}^{\varphi(n)} a_k = Q_1 Q_2,$$

hence, since $Q_2 = 1$ and $Q_1 = -1$ when $n = 4$, $n = p^\alpha$, or $n = 2p^\alpha$, and $Q_1 = 1$ otherwise, we conclude

$$\prod_{k=1}^{\varphi(n)} a_k = \begin{cases} 0 & n = 1, \\ -1 & n = 4,\ p^\alpha,\ 2p^\alpha, \\ 1 & \text{otherwise.} \end{cases}$$

□

4 Wilson Primes

After proving Wilson's Theorem, one can naturally lead into the question "How many primes p have their square divide $(p-1)! + 1$?" One could continue this question onto having the n-th power divide $(p-1)! + 1$, but asking such a question would presently be pointless as no one has been able to answer the first question.

Definition 4.1. *We define a* ***Wilson prime*** p *to be a positive integer for which* $(p-1)! + 1$ *is divisible by* p^2.

The only known Wilson primes are 5, 13, and 563, it is however conjectured that their are infinitely many of them. In fact, while it is conjectured that there are infinitely many of them, it is shown computationally in [3] that if there exist any more Wilson primes, then they all must be greater than $5 \cdot 10^8$. Wilson's Theorem is quite a isolated theorem in number theory, and as such no real progress has been made towards the answer of Wilson primes. One can see the importance of neighboring theorems when we look at Wieferich primes, which extend Fermat's little theorem in the exact same manner. While it hasn't been shown that there are infinitely many Wieferich primes, there are many more easily derivable properties Wieferich primes satisfy.

5 Conclusion

While Wilson's Theorem is quite isolated, it can be generalized extensively, becoming on its own right a powerful result about numbers. It has also sparked interest in a new set of primes, which like many set of primes, very little is known, and in this case all is conjecture. What Wilson first recognized and Gauss extended was a very clear relationship between the primality of a number and the product of its important predecessors.

References

[1] Artin, M. *Algebra*. Prentice Hall, New Jersey, 1991.

[2] Childs, L. N. *A Concrete Introduction to Higher Algebra*. Springer-Verlag, New York, 1995.

[3] Crandall, R., Dilcher, K., and Pomerance, C. A search for wierferich and wilson primes. *Mathematics of Computation 66*, 217 (January 1997), 433 – 449.

[4] Lang, S. *Undergraduate Algebra*. Springer-Verlag, New York, 2005.

[5] Nagell, T. *Introduction to Number Theory*. Chelsea, New York, 1964.

[6] Ore, O. *Number Theory and its History*. McGraw-Hill, 1948.